**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

--------------------------------------------------------------x

| | | |
|---|---|---|
| INTELLECTUAL VENTURES II LLC, | : | |
| Plaintiff, | : | |
| v. | : | 1:13-cv-03777-AKH |
| JP MORGAN CHASE & CO., JPMORGAN CHASE BANK, NATIONAL ASSOCIATION, CHASE BANK USA, NATIONAL ASSOCIATION, CHASE PAYMENTECH SOLUTIONS LLC and PAYMENTECH LLC | :<br>:<br>: | |
| Defendants. | : | |

--------------------------------------------------------------x

## INTELLECTUAL VENTURES II LLC'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

### CASES

## I. INTRODUCTION

Far from abstract, the ’694, ’409 and ’084 patents are directed to novel, innovative, and specific applications that JPMC uses to secure its electronic infrastructure. Stated plainly, there is nothing abstract about the patents at issue. The Supreme Court has explained that “abstract” means something that is a “building block[] of human ingenuity,” a “fundamental . . . practice,” a “principle,” “original cause,” or “motive.” *Alice Corp. Pty. v. CLS Bank Int’l*, -- U.S. --, 134 S. Ct. 2347, 2355 (2014). The dictionary defines “abstract” as “relating to or involving general ideas or qualities rather than specific people, objects, or actions.” Day Declaration ¶3, Ex. A. The ’694, ’409 and ’084 patents do not come close to meeting these definitions. They are specific inventions.

The ’694 patent is directed to a specific technique for filtering computer network packets by selecting and implementing access rules based upon the combination of the contents of received packets. ’694 patent, claim 1. The ’409 patent is directed to a cryptographic feature that protects each and every access to the unencrypted form of encrypted data according to rules enforced by an access mechanism. ’409 patent, claim 1. And the Patent Office has already found this feature as distinguishing the invention of the ’409 patent from the prior art in multiple *Inter Partes* Review petitions filed by IBM and banks plotting with JPMC. Day Declaration ¶4-6, Exs. B, C, D. Finally, the ’084 patent is directed to a network detection technique to monitor multiple data streams in order to detect anomalous behavior and then report that behavior. ’084 patent, claim 1. These are technological inventions that JPMC uses to electronically fortify its operations, not just boundless, abstract concepts.

Summary judgment is only appropriate when there are no genuine disputes of material facts. And despite only being able to file one summary judgment motion, JPMC filed its sole summary judgment motion before the close of fact discovery, before the close of expert discovery, and with no evidence in support of its argument. Section 101 is ultimately a question of law, but it is one that is prevailing with factual issues. JPMC's motion is entirely attorney supposition. It attaches no expert declaration to support its points. It never even analyzes why any of the ideas are abstract, and it ignores the Supreme Court's guideposts provided in *Alice Corp.* JPMC simply tells the Court the ideas are abstract and leaves it at that. Despite citing numerous cases in its Legal Background, it never even attempts to apply these cases to the facts here. It cannot explain why the ideas are abstract because the they are not. They are not long-standing, long-prevalent fundamental precepts. They are not things that can be done entirely in the human mind or on pen and paper. They are not merely conventional tasks without regard to specific technology or specific structure.

Most problematic, JPMC makes no argument that the patents entirely preempt any abstract idea. In *Alice*, the Supreme Court was clear that pre-emption "undergirds our § 101 jurisprudence." *Alice Corp.*, 134 S. Ct. at 2358. JPMC barely mentions this tenet in passing and never applies it to the facts here. It never attempts to argue that the claims preempt the entirety of any abstract concept. That is because the pre-emption analysis demonstrates why the challenged patents are valid; it shows the patent claims to be cabined to meaningful applications. This by itself precludes a finding in favor of JPMC.

JPMC also ignores what the patents' specifications and the claims as a whole. Rather, it parses the limitations into pieces, and incorrectly proclaims, without support, that IV's patents use "conventional" or "generic" computers. This is not true—the patents-in-suit do not claim abstract ideas to be run on "conventional computers" as discussed above. But more importantly, it is only when the claims—when "viewed as a whole"—recite an abstract idea and do nothing more than say "apply it with a computer," that they fail to meet the threshold inquiry of § 101. *Alice Corp.*, 134 S. Ct. at 2355-56. IV's patents are not directed to bare ideas that are just to be applied with a computer.

Only by repeatedly eschewing the Supreme Court's teachings, ignoring what the patents actually say, and making attorney argument without support, can JPMC argue the claims are invalid under § 101.

This is JPMC's one shot at summary judgment and because its motion is ill founded and ill conceived, it should be denied.

## II. LEGAL BACKGROUND

JPMC bears the burden of proving that the patents-in-suit claim ineligible subject matter under § 101. Like all issues of invalidity, JPMC must demonstrate that the patents are ineligible by clear and convincing evidence. *CLS Bank Int'l v. Alice Corp. Pty.*, 717 F.3d 1269, 1304 (Fed. Cir. 2013) ("We believe, moreover, that application of this presumption and its attendant evidentiary burden is consistent with the Supreme Court's admonition to cabin the judicially created exceptions to Section 101 discussed above."). In resolving this inquiry, the Court must construe "the evidence in the light most favorable to the non-moving party and draw[ ] all reasonable inferences in that party's favor." *Sledge v. Kooi*, 564 F.3d 105, 108 (2d Cir. 2009). Because JPMC bears the burden, it "must submit such clear and convincing evidence of facts underlying invalidity that no reasonable jury could find otherwise." *SRAM Corp. v. AD–II Eng'g, Inc.*, 465 F.3d 1351, 1357 (Fed. Cir. 2006). Failure to submit any support, other than attorney argument, even the context of § 101, precludes a party from succeeding on summary judgment. *Helios Software, LLC v. SpectorSoft Corp.*, No. 12-081, 2014 WL 4796111, at *17 (D. Del. Sept. 18, 2014) (finding that a moving party cannot show claims are drawn to an abstract idea when it "has provided no support for that position").

While ultimately an issue of law, § 101 is a question of law, it is one that is rife with factual inquiries.[1] *CLS Bank Int'l*, 717 F3.d at 1282-83, 1298-1302. Such inquires include whether the patent embraces an idea that can be described as abstract, whether it preempts or ties up any abstract idea, and whether the claimed limitations were indeed routine or conventional at the time of the patent's invention. *Id.*

Unlike other patent sections concerning invalidity, section 101 is a "coarse filter" because "the concern that drives th[e] exclusionary principle [is] one of pre-emption." *Alice Corp.*, 134 S. Ct. at 2354. Specifically, the concern is pre-emption where use of the claimed invention "would effectively grant a monopoly over an abstract idea." *Bilski v. Kappos*, 561 U.S. 593, 611-12 (2010). But, as the Supreme Court has repeatedly cautioned, courts must "tread carefully in construing the exclusionary principle [of § 101] lest it swallow all of patent law." *Alice Corp.*, 134 S. Ct. at 2354 (citing *Mayo*, 132 S. Ct. at 1293-94). This is because "[a]t some level, all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." *Id.* (quoting *Mayo*, 132 S. Ct. at 1293). And it is clear that "applications" of such concepts are patent eligible. *Id.*; *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972).

Determining whether claims are patent-ineligible under a § 101 inquiry is a two-step process. First, the Court must determine "whether the claims are directed to a patent-eligible concept." *Alice Corp. v. CLS Bank Int'l*, 573 U.S. –, 134 S. Ct. 2347, 2355 (2014). This requires identifying whether the patent claims a law of nature, a natural phenomena or an abstract idea, as opposed to a "patent-eligible application of those concepts." *Id.* Only if the claims are directed to a patent-ineligible concept is the second inquiry considered. *Id.* In *Alice Corp.*, the Supreme Court described abstract ideas as "building blocks of human ingenuity," a "fundamental . . .

[1] JPMC failed to submit a statement of material facts as per Local Civil Rule 56.1.

practice," a "principle," "original cause," or "motive." *See Alice Corp.*, 134 S. Ct. at 2354-57; *Mayo*, 132 S. Ct. at 1294; *see also Bilski v. Kappos*, 130 S. Ct. 3218, 3229-32 (2010); *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972). In earlier cases, the Court addressed abstract ideas such as bare mathematical formulas or algorithms. *See Diamond v. Diehr*, 450 U.S. 175, 192-193 (1981) (mathematical formula by itself was abstract, but not when used meaningfully for computing cure time in rubber-molding presses); *Parker v. Flook*, 437 U.S. 584, 594-95 (1978) (mathematical algorithm for computing alarm limits); *Benson*, 409 U.S. at 71-72 (mathematical algorithm for converting binary decimal numbers into pure binary form). The guideposts established by the Supreme Court, and applied by this Court, include (1) whether the idea at issue was long-standing and fundamental; (2) whether the idea can be practiced entirely in the human mind or on pen and paper; and (3) whether it is a conventional idea without reference to specific technology or structure. *Alice Corp.*, 134 S. Ct. at 2355-56; *Mayo*, 132 S. Ct. at 1294; *Bilski*, 130 S. Ct. at 3229-32; *DietGoal Innovations LLC v. Bravo Media LLC*, No. 13-8391 PAE, -- F.Supp.2d --, 2014 WL 3582914, at *10-11 (S.D.N.Y. July 8, 2014).

The second inquiry "considers the element of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Id.* (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. – , 132 S. Ct. 1289, 1297-98 (2012). Thus, the claims must be considered as a whole as well as by their individual limitations. *Id.* (citing *Diehr*, 450 U.S. at 188). "Any claim can be stripped down, simplified, generalized, or paraphrased to remove all of its concrete limitations, until at its core, something that could be characterized as an abstract idea is revealed…A court cannot go hunting for abstractions by ignoring the concrete, palpable, tangible limitations of the invention the patentee actually claims. *CLS Bank Int'l v. Alice Corp. Pty.*, 717

F.3d 1269, 1298 (Fed. Cir. 2013).

Considering the claims as a whole, and as written, the Court searches "for an 'inventive concept'—*i.e.*, an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself." *Id.* (quoting *Mayo*, 132 S. Ct. at 1294). In this regard "*Mayo* made clear that transformation into a patent-eligible application requires 'more than simply stat[ing] the [abstract idea] while adding the words 'apply it.'" *Id.* (quoting *Mayo*, 132 S. Ct. at 1294). Moreover, "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Alice Corp.*, 134 S. Ct. at 2358.

## III. ARGUMENT

### A. The '694 Patent Does Not Claim an Abstract Idea

1. <u>The Invention of the '694 Patent</u>

The '694 patent was filed in 1998 by AT&T and is entitled "High Resolution Access Control." Malicious software ("Malware"), such as a virus, is often disguised as something else or buried within a file that appears recognizable and safe. When a file or program is transmitted over a network it is broken up into small packets, somewhat like the pieces of a puzzle, and the packets themselves are routed from a source, over the network, to a destination, where the packets may be reassembled.

A packet has at least two distinct segments or portions, a header and a payload. '694 patent, 2:22-23. A packet header includes header parameters, such as source address, source port, destination address, destination port, and protocol number. *Id.* at 2:26-29. The address information gets the packet to its destination. The protocol number, and some of the other header parameters, are needed to decode and make sense of the packets once they arrive, as are some of the other header parameters listed. The payload includes the data to be conveyed by the packet from its source to its intended destination. *Id.* at 1:26-28.

The ’694 patent uses a filter (such as a firewall) to filter out packets as they travel from a source to a destination. *Id.* at 1:40-44. It can do this based upon many different factors and multiple rules. A rule may be just a pass drop (Fig. 1, step 104) or may call for referral to an access control proxy (Fig. 1, steps 103, 105), which is used to analyze the content within a packet payload (Fig. 1, step 106). Based upon this *high-resolution* payload based analysis, an appropriate rule is selected and implemented to filter packets (Fig. 1, steps 107, 108). A high-resolution rule may also be formulated based upon a deep inspection of multiple packets. The access control proxy analyzes the contents of a plurality of received packets to determine details pertaining to a request for information that is constituted by the plurality of payloads. The number of packets analyzed is sufficient to select an access rule pertaining to the detailed information request. *Id.* at 3:23-29. In other words, the proxies can perform a high-resolution deep packet inspection and piece together what the puzzle may be and select a rule based upon the inspection.

### 2. <u>The ’694 Patent is Not Directed or Drawn to an Abstract Idea</u>

That fact that the ’694 patent is not directed to an abstract idea is underscored by JPMC’s failure even to identify what it contends the abstract idea of claim 1 is. But identifying the “abstract idea” is the first step in the two-step inquiry outlined by the Supreme Court in *Alice*. Nevertheless, JPMC ignores it altogether. *Alice Corp.*, 134 S. Ct. at 2355; *Helios Software, LLC v. SpectorSoft Corp.*, No. 12-081, 2014 WL 4796111, at *17 (D. Del. Sept. 18, 2014) (finding that a moving party cannot show claims are drawn to an abstract idea when it “has provided no support for that position”).

JPMC did not identify an abstract idea because the ’694 patent is directed to a novel and specific technique for filtering packets in a computer network and not some broad and boundless abstract idea. *See Alice Corp.*, 134 S. Ct. at 2359. The patent is the antithesis of abstractness.

Indeed, the ’694 patent does not cover all methods of transmitting computer network packets; which itself is not an abstract concept. It also does not cover all methods of filtering computer network packets. To the contrary, the ‘694 patent distinguishes its claimed method from the filtering methods covered by the prior art. *See, e.g.*, ’694 patent, 1:58-63, 2:6-10. Thus, “the pre-emption concern that undergirds our § 101 jurisprudence” is wholly absent and the ’694 patent is not directed to any abstract idea. *Alice Corp.*, 134 S. Ct. at 2354-55 (stating that as between abstract ideas and “something more” that “the former would risk disproportionately tying up the use of the underlying ideas, and are therefore ineligible for patent protection. The latter pose no comparable risk of pre-emption, and therefore remain eligible for the monopoly granted under our patent laws.”) (internal quotations and citations omitted). It was this same concern that animated all of the Supreme Court’s § 101 jurisprudence. See *Mayo*, 132 S. Ct. at 1294-98; *Benson*, 409 U.S. at 71-72; *Parker v. Flook*, 437 U.S. 584, 594-95 (1978). Tellingly, JPMC never addresses the pre-emption inquiry, nor does JPMC raise a pre-emption issue because there is none.

Rather than claim an abstract idea, the ’694 patent claims a specific technique for filtering computer packets by selecting and implementing access rules based upon the combination of the contents the payload of a received packet as well as the contents of another packet or packets. ’694 patent, claim 1. This is an extremely important technique. The information needed to select and implement the rule may be strategically fragmented and hidden in multiple packets in order to make it difficult to detect. Further, pre-selected and implemented rules are inadequate to protect against ever changing threats within those packets. The ’694 patent thus enables filtering of unwanted material that would otherwise be unfiltered if the conventional practice, that did not use a the combination of the contents of multiple packets, was implemented. *See*, *e.g.*, ’694 patent, 5:1-24. Indeed, as explained by the ’694 patent, filtering in this specific way “advantageously provides a more efficient, flexible and scalable system and method for implementing the rules of a security policy or policies at a filtering device, because a rule is *only loaded at the filtering device when the rule is needed*.” ’694 patent, 6:29-34 (emphasis added).

Just as pre-emption is not a concern with the ’694 patent, nor are any of the other guideposts that would suggest the claimed idea is abstract. JPMC offers no evidence that the computer packet filtering technique claimed by the ’694 patent is a “building block[] of human ingenuity.” *Alice Corp.*, 134 S. Ct. at 2355-56. This Court has been careful to follow the Supreme Court’s teachings with regards to § 101. In *DietGoal Innovations LLC v. Bravo Media LLC*, No. 13-8391 PAE, -- F.Supp.2d --, 2014 WL 3582914, at *10 (S.D.N.Y. July 8, 2014), the Court discussed *Alice Corp.* and its progeny at length. There, the patent at issue was directed to an abstract idea of meal planning. The patent was for a computer program that helped a user plan meals based on nutrition needs. *Id.* at *2. In deciding that the idea was abstract, the Court relied on three primary guideposts. First, “meal planning” was a “long prevalent practice” at least as old as hedging and intermediated settlement. *Id.* Second, the concept could “be performed in the human mind, or by a human using a pen and paper.” *Id.* One could sit down, as one had done for centuries and plan a meal based on their needs. Third, the claims were directed to “conventional and quotidian tasks” that could be performed “without the aid of any particular or structured method and without the need of any technology.” *Id.*

None of the same can be said of the ’694 patent. There is no evidence of a long-standing, decades old, fundamental precept of filtering computer packets by selecting and implementing access rules based upon the combination of the contents of the payload of received packet as well as the contents of another packet or packets. *Id.*; '694 patent, at claim 1. Yet these are the limitations required to practice the invention. '694 patent, claim 1. There is no evidence that the patent can be performed in the human mind. It cannot. The claimed packet is nothing like, nor is it even comparable to, the "slips of paper" that JPMC would have the Court believe could be used to practice the invention. Motion at 10. JPMC's "slips of paper" analogy is not even apt as there is no reason to design or use the technique that AT&T developed in the absence of electronic information that is packetized. No one decides whether slips of paper can have access[2] based upon rules from the contents of packets drawn on paper. The fact that JPMC has to say that the "slips of paper" would have "packets written on them" only shows that the invention can be *described* on paper (as all inventions are and all patents must be) and belies the assertion that it can be *performed* on paper by a person or that there is utility in trying to perform it on paper. The technique of the '694 patent technique is novel to the only context in which it applies—networked computing. Thus, the *CyberSource* case that JPMC cites—which deals with claims that can be performed by a person in their mind—is inapposite. *CyberSource Corp. v. Retail Decisions*, 654 F.3d 1366 (Fed. Cir. 2011).

Furthermore, claim 1 is not directed to conventional tasks without any particular structure or technology. JPMC's only argument that the '694 patent claims an abstract idea is because the claim 1 does not require a computer and that a person could perform the claim. Motion at 10. Not true. A person cannot receive a computer network packet without a computer. Nor can a person decode the electrical signal that represents the data of the packet, and then analyze the header or the payload of such a packet without a computer. Finally a person cannot implement

[2] To what JPMC believes slips of paper would be analyzed for access is unexplained and remains anyone's guess.

filtering rules based upon the analysis and filter computer network packets without a computer. The Court has already ruled that the packet filtering described by and claimed in the ’694 patent is computer network based. D.I. 82 at 11 (construing “packet” as “discrete unit of information being routed through a computer network, often to a designated addressee”). And any fair reading of the ’694 patent clearly shows that what is described and claimed is a specific way to filter in that computer-network environment. Moreover, the ‘694 patent does not claim just any computerized packets; rather, the received packets must have at least one header parameter and payload that are used to select an access rule that is implemented based upon the combination of those contents and the contents of the payload of a separate packet. ’694 patent, claim 1.

JPMC’s argument rests entirely on removing multiple claim limitations and making an inapt analogy to raise an issue of abstractness. A specific technique for filtering packets in a networked computer based upon the implementation of rules that are selected by a combination of the contents of the payloads of multiple packets is not abstract. JPMC ignores the teachings of *Alice Corp.* and all of the cases it discusses in its legal background, failing to apply them to the facts here. In so doing, it fails to meet its burden to prove invalidity by clear and convincing evidence. *CLS Bank Int’l*, 717 F.3d at 1304.

### 3. Assuming The ’694 Patent Claims An Abstract Idea (It Does Not), The Claimed Limitations Recite Significantly More

Because no abstract idea is actually claimed, the Court’s analysis need go no further. The second inquiry set forth in *Alice* applies only if the ’694 patent claims an abstract idea. *Alice Corp.*, 134 S. Ct. at 2355. Even assuming it did, however, claim 1 is directed to an innovative concept where packets in a computer network are filtered using a specific technique, making the ’694 patent eligible under § 101.

Step two of the § 101 test (assuming it applies) “examine[s] the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice Corp.*, 134 S. Ct. at 2357 (quoting *Mayo*, 132 S. Ct. at 1294, 1298). Here, the '694 patent is meaningfully limited to an application and provides an inventive concept that adds significantly more to any broad concepts at issue. As explained above, the patent does not pertain to all methods of transmitting computer packets, all methods of filtering computer packets, or even all methods of filtering computer packets based upon packet headers and packet payloads. Instead, it is meaningfully limited to the scenario where the packets are filtered based upon rules that are selected and implemented based upon the analysis of the contents of the payloads of multiple packets. '694 patent, claim 1. This solves the problem of analyzing packets where the basis for selecting and implementing the rules is spread out across multiple packets, and allows for new rules to be loaded as necessary. JPMC, however, ignores these meaningful limitations to argue there is nothing more in the claim than an abstract idea. Motion at 10-12.

The meaningfulness of the limitation of claim 1 of the '694 patent is buttressed by the specification's teaching of "a *specific way* of doing something with a computer." *CLS Bank Intern. v. Alice Corp. Pty. Ltd.*, 717 F.3d 1269, 1302 (Fed. Cir. 2013) (emphasis in original).[3] In this regard, "[a] special purpose computer, *i.e.*, a new machine" is something that is "specially designed to implement a process" and may be sufficient under § 101. *Id.* (citing *In re Alappat*, 33 F.3d 1526, 1545 (Fed. Cir. 1994) (holding that "programming creates a new machine, because a general purpose computer in effect becomes a special purpose computer once it is programmed to perform particular functions pursuant to instructions from program software"). Here, the

[3] The Supreme Court discussed in its opinion that one cannot save a claim to an abstract idea by simply stating "apply it with a computer" (*Alice Corp.*, 134 S. Ct. at 2358) and left undisturbed the discussion in Judge Rader's opinion concerning a specific machine.

"patent does more than simply instruct" one to perform an abstract idea "on a generic computer." *Alice Corp.*, 124 S. Ct. at 2359. It teaches using a specific system—*i.e.*, one that performs a method of packet filtering with rules that are selected and implanted based upon the payload contents of multiple packets. Neither these steps nor the technology itself were "purely conventional" at the time the patent was filed, nor is there any evidence that they were conventional. *See id.*

JPMC's arguments that the '694 patent claims nothing more than an abstract idea all fail. JPMC asserts that claim 1 adds nothing more to its unidentified abstract idea because "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." Motion at 10-11; *see Alice Corp.*, 134 S. Ct. at 2358-59. Again, JPMC's conclusion is supported by attorney argument only. And while a generic computer cannot save an otherwise ineligible claim, it is inapplicable here because it assumes the '694 patent claims an abstract idea, which it does not as described above. Moreover, it assumes the '694 patent is implemented by a generic computer. It is not. As described above, a network-based system with the ability to perform such filtering techniques is not a general-purpose computer.

JPMC further argues that because the '694 patent makes use of components that were known at the time of the invention, the '694 patent cannot pass scrutiny under § 101. This is not the law. All technologies build on themselves. Computer technology takes what is in the field and improves on it as well.[4] This is the nature of invention generally. To follow JPMC's argument through logically, there can be no invention, there can be no patents, because if, at bottom, the invention is founded on an idea, then it is ineligible. There is no patent currently

[4] Consider, for example, pharmaceuticals. All pharmaceuticals make use of known, previously existing, elements in nature but no one would claim that all pharmaceutical advances are patent ineligible because they "simply" combine "known elements."

issued or before the Patent that cannot be found ineligible by JPMC's delimiting analysis. The '694 patent uses known components in a way that are novel and useful; it innovates and furthers the art. Even if it used "known firewalls" or even known computer technology, there is no dispute that AT&T developed a specific method of filtering packets, rather than an unbounded abstract idea. Arguing that the claims just use known components (as JPMC has done) is to argue that the '694 patent is invalid under § 102 (anticipation) or § 103 (obviousness) (which it is not) but not § 101 (patent eligibility). In this regard, all of the cases cited by JPMC at pages 4-8 of its Motion are inapposite.

JPMC also argues that "the alleged improvement [of the '694 patent] lies in the *idea* of selecting the access rules based upon the information in the payload—*not* in any particular machine or specific program for implementing that idea." Motion at 11 (emphasis in original). This argument is wrong, irrelevant, and ignores the limitations of the claimed invention. All improvements stem from ideas, but that does not make them patent ineligible. It is this perilous type of inquiry that the Supreme Court warned against when it cautioned courts to "tread carefully in construing the exclusionary principle [of § 101] lest it swallow all of patent law." *Alice Corp.*, 134 S. Ct. at 2354 (citing *Mayo*, 132 S. Ct. at 1293-94). "At some level, all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." Id. (quoting *Mayo*, 132 S. Ct. at 1293).

Even putting aside JPMC's utter lack of proof, the claimed improvement of the '694 patent is not conventional at all.[5] It is more than just selecting access rules based upon

[5] JPMC's final argument that the '694 patent is invalid based upon statements found in the prosecution history is irrelevant. The fact that the patentee narrowed what became claim 1 during prosecution has no bearing on whether the '694 patent claims an abstract idea; to the contrary, the fact that the patentee narrowed the claim of the patent during prosecution demonstrates the specific and concrete nature of the claim.

information in the payload. It is selecting and implementing the access rules based upon a combination of the contents of payloads of multiple packets. Finally, the assertion that this invention is not "any particular machine or specific program" is belied by the claim. Only a particular machine with a specific program can carry out the method that is claimed, as packets have never been filtered in this way before. There are many different types of computers, and the '694 patent has claimed a specific type of computer—a novel one that filters packets in a new and useful way. This is the definition of a new, special purpose computer. New methods for computer packet filtering cannot be abstract—they are concrete and fixed implementations.

JPMC repeatedly ignores what the specific technique claimed by '694 patent is to forge its § 101 arguments. This is improper and highlights why JPMC's assertion of patent ineligibility fails.

### B. The '409 Patent Does Not Claim an Abstract Idea

#### 1. The Invention of the '409 Patent

The specification of the '409 patent is clear, and the Court has already held that the '409 patent is directed to, among other things, controlling the distribution of, and access to, digital property, using the cryptographic arts. In essence, the '409 patent claims a method of providing continued protection after a file is initially decrypted. *See, e.g.*, D.I. 82 at 6,[6] 7,[7] 8.[8] Prior to the '409 patent "access [was] all or nothing, that is, once access is granted, it cannot be controlled in any other ways" and there was nothing that "limit[ed] either secondary distribution or

[6] "The patent is a method for limiting access to sensitive data. Sensitive is encrypted and then sent with rules limiting who can access the data. (The rules can also be sent and/or stored separately.) A computer gives access to the dat[a] in an unencrypted form as provided for by the rules. Different people may be given different access to data, for different purposes."

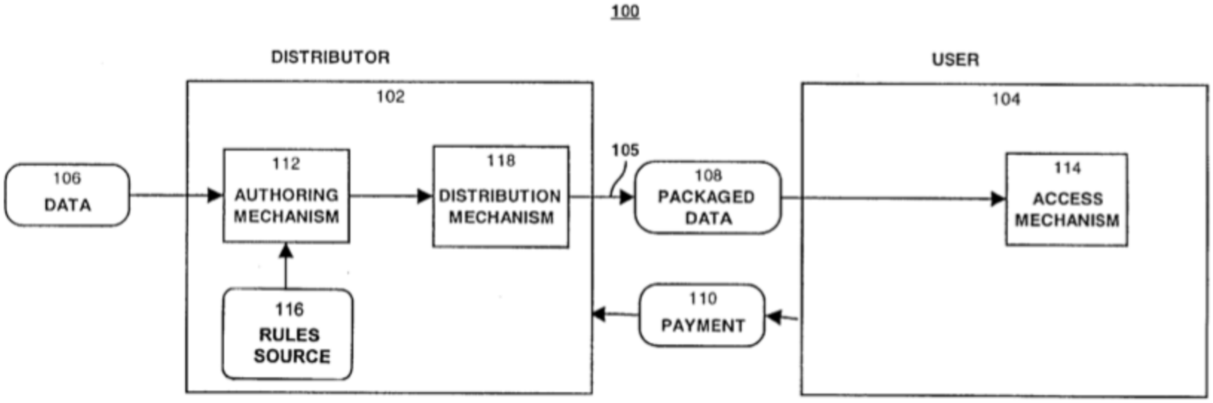
[7] Construing "protected portions of the data" as "encrypted portions of the data."

[8] Construing "unprotected form of the protected portions of the data" as "unencrypted form of the protected portions of the data"; construing "access mechanism" as "hardware and/or software for controlling access to data."

distribution of derivative works." '409 patent, 3:62-65, 4:65-5:3. This failure of prior systems was due to "an architectural design omission in the art." *Id.* at 5:4-6. The omission was an architectural design that did not prevent data from being "copied, modified or transmitted at will" after the data was initially "made available to [a single] authorized user." *Id.* at 5:6-11. Thus, secondary distribution was not prevented and sensitive data could be "freely manipulated and redistributed" after initially becoming available in unencrypted form. *Id.* at 5:13-16. Secondary distribution refers to further distribution after the initial user has received the file.

The '409 patent solved this problem and fundamentally changed how sensitive encrypted data is distributed in order to prevent unauthorized access. Figure 1 depicts one embodiment of the invention:

*FIG. 1*



As depicted above, the system (100) includes a data distributor (102) and a user (104). *Id.* at 9:51-58. The data distributor sends packaged data (108) to the user via a communication channel (105). *Id.* The packaged data may include an encrypted body part (120) and an unencrypted body part (122). *Id.* at 10:48-53.

Rules that control access to the packaged data can either be encrypted and packaged with the data or provided separately. *Id.* And an access mechanism permits the user access to the data in the packaged data according to the rules and "prevents the user or anyone else from accessing the data other than as allowed by the rules." *Id.* at 15:30-35. Some example rules are rules that control local display rights, printing rights, copying rights, execution rights, transmission rights, and modification rights to the data. *Id.* at 23:15-65. In Figure 8 of the '409 patent, an embodiment of the access mechanism is depicted as having various components including, among other things, a processing until, memory and encryption hardware and related software. *Id.* at 15:41-49.

The '409 patent also describes in detail and claims controlling secondary distribution of data in its unprotected (unencrypted) form. '409 patent, 25:60-62. One way this is achieved is through an architecture where an unencrypted copy of the data is transmitted under the direction of "rules embodied in the owner's permission list." *Id.* at 25:63-67.

### 2. The Claims of the '409 Patent Are Not Directed or Drawn to an Abstract Idea

Contrary to JPMC's assertions, claim 1 of the '409 patent is not "directed to the abstract idea of restricting access to data using a set of rules" or "the idea of controlling access to openly distributed information." Motion at 12. Nor are these abstract ideas. The key novel aspect of the '409 patent is not just that the invention encrypts and decrypts data, restricts data using rules, or controls access to openly distributed information. Rather, the invention is directed to controlling access and distribution of sensitive encrypted data even after it has been encrypted. Protecting data such that "each and every access to the unprotected [i.e., unencrypted] form of the protected portions of the data is limited in accordance with rules defining access rights to the data as enforced by an access mechanism" was neither taught or suggested by the prior art and was the problem that the inventors of the '409 patent solved. '409 patent, claim 1.

The PTO has also recognized the proper scope of the ’409 patent. JPMC, IBM and a number of banks have tried to invalidate the 33 asserted claims of the ’409 patent with numerous pieces of prior art in four petitions for *Inter Partes* Review (“IPR”), and have had a resounding lack of success. Despite their multiple attempts to invalidate the ‘409 patent, JPMC, IBM and others have only been able to demonstrate a “reasonable likelihood” that a single claim—claim 23—of the ‘409 patent is invalid. Day Declaration ¶¶4-6, Exs. B, C, D.[9] Moreover, the Patent Office expressly found that the patent claims protecting each and every access to the unencrypted form of the encrypted data according to rules enforced by an access mechanism and that this distinguishes the invention from the prior art. Day Declaration ¶4-6, Ex. B (Decision on IPR2014-00672 at 9-13), C (Decision on IPR 2014-00673 at 10-13), D (Decision on IPR 2014-00719 and 2014-00722 at 12-15). This finding in and of itself shows that that the ’409 patent does not raise pre-emption concerns as is, is not directed to a long-standing, prevalent practice, and is thus not directed to an abstract idea. *McRO, Inc. v. Atlus U.S.A.*, No. 13-1870, 2014 WL 4772196, at *8 (C.D. Cal. Sept. 22, 2014) (“It is hard to show that an abstract idea has been preempted if there are noninfringing ways to use it in the same field.”). While the broad concept of “access to data based upon rules” has been around for many years, JPMC, IBM and numerous banks cannot find a single reference that is “reasonably likely” to suggest that claims are invalid under § 102 (anticipation) or § 103 (obviousness), much less the “coarse filter” of § 101 (patent eligibility). *Alice Corp.*, 134 S. Ct. at 2354.

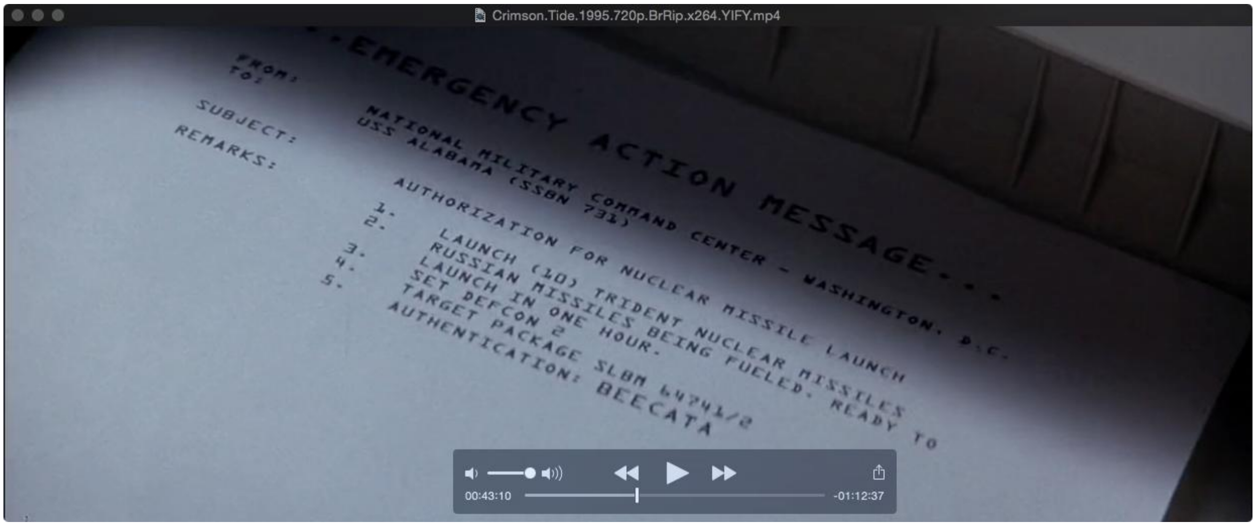
None of these concepts identified are abstract. Even the ideas articulated by JPMC—

[9] JPMC, IBM and the other banks were only able to convince the Patent Office that there was a “reasonable likelihood” that claim 23 was invalid in light of prior art. While IV does not agree that claim 23 is invalid under § 101 or in light of prior art, nor has such determination been made that is final or binding, IV hereby drops claim 23 from this case in order to keep this case efficiently moving towards resolution.

being directed to restricting access to data using a set of rules or the idea of controlling access to openly distributed information—are abstract. Again, JPMC fails to provide any analysis that these are abstract in comport with the Supreme Court's holding in *Alice Corp.* JPMC offers no evidence that the '409 patent's solution to the problem of secondary distribution and access to decrypted data is a "building block[] of human ingenuity." *See Alice Corp.*, 134 S. Ct. at 2355. There is also no evidence of a long-standing, decades old, fundamental precept of the feature that protects each and every access to the unencrypted form of encrypted data according to rules enforced by an access mechanism. *Id.*; '409 patent, claim 1. It cannot be practiced entirely in the human mind or on pen and paper. And it is not merely conventional activity without regard to structure or technology. JPMC's arguments do not contradict these points.

Here too JPMC offers no evidence that there is a pre-emption concern, despite this being the paramount concern underlying § 101 ineligibility. There are many ways to control distribution and access to sensitive data that is encrypted. The '409 patent claims just one of those ways, through it is an extremely novel and now ubiquitously used way. JPMC does not argue that the '409 patent preempts all ways of controlling access to or encrypting data. Further, the PTO has already found that the '409 patent is distinguished from the related art. Relatedly, JPMC makes the argument in passing on page 14 of its brief that because the claim recites an "access mechanism" it somehow preempts the field. Motion at 14. Nonsense. If that were true the Patent Office would not have found all of these claims valid over the prior art asserted by JPMC, IBM and the other banks. These claims only preempt what is claimed: a specific way of controlling access and distribution of digital property through encryption. Every patent pre-empt what it claims. *Alice Corp.*, 134 S. Ct. at 2354-55.

Perhaps realizing that it has over simplified the claim—by ignoring most of the limitations—to create an abstract idea, JPMC makes an incorrect and inapt analogy to a movie (*Crimson Tide*), the facts of which, JPMC misrepresents. First, the message in the movie was never encrypted. Rather, the message was delivered in plain text as can be seen here in a screen shot from the movie:



..EMERGENCY ACTION MESSAGE...

FROM: NATIONAL MILITARY COMMAND CENTER - WASHINGTON, D.C.
TO: USS ALABAMA (SSBN 731)
SUBJECT: AUTHORIZATION FOR NUCLEAR MISSILE LAUNCH
REMARKS:
1. LAUNCH (10) TRIDENT NUCLEAR MISSILES
2. RUSSIAN MISSILES BEING FUELED. READY TO
LAUNCH IN ONE HOUR.
3. SET DEFCON 2
4. TARGET PACKAGE SLBM 64741/2
5. AUTHENTICATION: BEECATA

Thus, the message was never encrypted and then subsequently decrypted by Mr. Washington, as raised by JPMC. Second, the alleged "military regulations" that JPMC cites that supposedly required Mr. Washington to destroy the original message were promulgated by the Department of Homeland Security and did not exist until 2004, nine years after the move was released. Day Declaration ¶ 7, Ex. E. On page 13 of its brief JPMC argues "[t]he only thing the claims adds to the *Crimson Tide* version is the idea of replacing a Hollywood movie star with a computerized 'access mechanism.'" Motion at 13. Neither Mr. Washington, nor any human being, can carry out this claim. In order to protect each and every access to the unencrypted form of the encrypted data according to enforced rules enforced, a computerized system is necessary because a person cannot prevent further unauthorized access or distribution after decryption. Because JPMC could not find any long standing practice that is anything like the '409 patent, it had to 1) analogize to a Hollywood movie; 2) misrepresent the facts of the movie;

and, 3) existence of a regulation that was "not shown in the movie" because it did not exist until *nine years* later.

But putting all of this aside, and assuming JPMC's account of the movie is accurate (it is not), JPMC's analogy does nothing to show that claim 1 of the '409 patent is abstract. It is certainly narrower and different than what was shown in *Crimson Tide*. The entire point of the '409 patent is to control access to and distribution of the unprotected unencrypted form of previously encrypted data. '409 patent, 35:37-43. Directing an individual to voluntarily throw away or destroy unencrypted data does not achieve this goal. If Mr. Washington actually decrypted the message and provided to Gene Hackman's character (as JPMC claims), the majority of the claim is not even practiced by JPMC's analogy because the decrypted data could be distributed by Mr. Hackman. Again, this is the scenario that the '409 patent's inventors sought to, and did in fact, solve by protecting each and every access to the unencrypted form of the encrypted data according to rules enforced by an access mechanism. '409 patent, 35:37-43. If JPMC's analogy were factually accurate, Mr. Washington did the exact opposite of the invention by providing the unencrypted form of the message to Mr. Hackman without any secondary means of protection to further access or distribution. This was the problem the inventors sought to solve, not the claimed solution.

JPMC's analogy is also inapposite because it does not (and cannot) identify how each and every access to the unprotected form of the message is controlled in accordance with rules enforced by an access mechanism so that unauthorized access is not to the protected portion of the message from Naval Command. This is because once Mr. Washington unencrypts the message in JPMC's hypothetical, nothing prevents *further distribution*—*i.e.*, the problem solved by the '409 patent. '409 patent, 5:4-16.

The ’409 patent does not claim an abstract idea and JPMC has offered no analysis or evidence to suggest otherwise. Controlling access to distributed sensitive encrypted data in its unencrypted form is not abstract and not some fundamental practice.

### 3. Assuming The ’409 Patent Claims An Abstract Idea (It Does Not), The Claimed Limitations Recite Significantly More

Assuming for purposes of argument that the ’409 patent is directed to an abstract idea, it claims an inventive concept and “additional elements that transform the nature of the claim into a patent eligible application” under § 101. *Alice Corp.*, 134 S. Ct. at 2355. Here, the patentees were clear as to what the inventive concept is and it is expressly recited in various ways in the asserted claims.

The inventive concept is protecting each and every access to the unencrypted form of the encrypted data (*i.e.*, the unprotected form of the protected portions of the data) according to rules enforced by an access mechanism. ’409 patent, 35:37-43. The inventive concept is not the access mechanism in isolation,[10] “restricting access to data using a set of rules” in isolation, or “controlling access to openly distributed information” in isolation, as JPMC argues. Motion at 12-15. Rather, it is preventing an identified problem in the art (secondary access to, and distribution of, sensitive data) with a new and unique solution (protecting each and every access to the unencrypted form of the encrypted data according to rules enforced by an access mechanism). ’409 patent, 5:4-16, 35:37-43. This was an undeniable problem in the art and the patentees solved it. ’409 patent, 5:4-16. JPMC, however, has to ignore (1) the problem in the art and (2) the meaningful limitations in claim 1 that the patentees added to overcome the problem

[10] JPMC is grasping at straws to make its arguments. On page 13 of is brief JPMC argues that a single sentence from a draft IV presentation is some kind of concession that the only point of novelty of the ’409 patent is the “access mechanism.” It is not for all the reasons explained in this brief (including the reasons set forth by the inventors in the specification) and the reasons the Patent Office explained in rejecting four IPR petitions as to 32 of the 33 asserted claims. Day Declaration ¶4-6, Exs. B, C, D.

in the art in order to argue there is nothing more in the claim than an abstract idea. Motion at 12-15. JPMC cannot argue that a claim is abstract by ignoring the invention and the inventive concept altogether.

Further, in order to manufacture an abstract idea where there is none, JPMC has read out the novel limitation and more than half the claim. To draw its conclusion that claim 1 of the ’409 patent is directed what JPMC calls the “abstract idea of restricting access to data using a set of rules” or “the idea of controlling access to openly distributed information,” JPMC completely ignores the bolded portions of claim 1:

> 1. A method of distributing data, the method comprising:
>
> protecting portions of the data; and
>
> openly distributing the protected portions of the data, whereby
>
> ***each and every access to an unprotected form of the protected portions of the data is in accordance with rules defining access rights to the data as enforced by an access mechanism, so that the unauthorized access to the protected portions of the data is not to the unprotected form of the protected portions of the data***.

JPMC cannot find an abstract idea by ignoring the last limitation—and over half the claim—altogether.

That claim 1 of the ’409 patent requires each and every access to the unencrypted form of the encrypted data according to rules enforced by an access mechanism, buttresses the fact that the patentees claimed “a *specific way* of doing something with a computer,” and not an abstract idea. *CLS Bank*, 717 F.3d at 1302 (emphasis in original). Again, implementing this inventive concept in a networked system makes this the invention “[a] special purpose computer, *i.e.*, a new machine.” *Id*. (citing *In re Alappat*, 33 F.3d 1526, 1545 (Fed. Cir. 1994)). This not saying apply an idea with a generic computer. The ’409 patent teaches using a specific system: with rules enforced by an access mechanism. These steps, nor the technology itself, were “purely conventional" at the time the patent was filed, nor is there any evidence that they were conventional. *See id.* JPMC offers no evidence or expert support for any of its suppositions.

JPMC's argument that the '409 patent specification envisions using "a standard computer, equipped with an access mechanism 114 [that] will function as an authoring/distribution system" is irrelevant and does not support its argument that the claims are unpatenable. Motion at 13-14. First, this is no longer a standard component because it is using an access mechanism as claimed and taught by the patent. Even if it were standard, there is no prohibition on using standard components in order to develop a new invention. If there were, there could be no further invention in the art of computers after the first computer was made and clearly computers have come a long way. Nearly every invention ever made uses "standard parts" at some level. Inventions take the prior art, build upon it, and make something new, novel and useful. Section 101 only precludes the claiming of abstract ideas, with no inventive concept that do *nothing more* than say apply the idea or perform the idea on a computer. *Alice Corp.*, 134 S. Ct. at 2358-59. That is not the '409 patent. Here, for the reasons discussed above, the inventors of the '409 patent advanced the art of cryptographically distributing and controlling access to digital data. And the Patent Office agreed that they advanced the art multiple times. Day Declaration ¶¶4-6, Ex. B (Decision on IPR2014-00672 at 9-13), C (Decision on IPR 2014-00673 at 10-13), D (Decision on IPR 2014-00719 and 2014-00722 at 12-15).

JPMC's argument that internal IV documents show that the '409 patent covers a diverse set of technologies is irrelevant to the § 101 inquiry here. Motion at 14. The '409 patent does in fact cover any technology that, among other things, protects each and every access to the unencrypted form of the encrypted data according to rules enforced by an access mechanism, and that satisfies all other elements of the claim. '409 patent, claim 1. Broad applicability does not mean that a patent claims an abstract idea; it just means that there is rampant infringement. Billions of people have used the wheel in a broad range of contexts, but it does not mean the wheel was an abstract idea.[11] Moreover, it is not surprising that the ’409 patent has broad applicability because controlling secondary access to, and distribution of, digital data is a significant problem and the ’409 patentees developed a compelling solution.

JPMC’s remaining arguments just point to claim terms in isolation and say they add “nothing more” to transform claim 1 of the ’409 patent into a patent-eligible invention. Motion at 14-15. This is improper because the claims must be looked at as a whole. *Alice Corp.*, 134 S. Ct. at 2358. These arguments are also irrelevant because they ignore the inventive concept that is outlined in the specification, recited in the claims, and discussed above. Anyone can point to single claim limitations of any patent (eligible or not) and say that, in isolation, it “adds nothing more.” But that is not the proper inquiry. The proper inquiry is whether an abstract idea is claimed and, if not, whether there is an inventive concept such that the claim is significantly more than the idea itself. JPMC offers no evidence on either point.

#### 4. The Other Asserted Independent And Dependent Claims of The ’409 Patent Are Also Are Not Directed or Drawn to an Abstract Idea

The other asserted claims—claims 2-11, 13-21, 24-27, 29-30, 32-33, and 36-39—all pass the § 101 inquiry here for at least the same reasons as claim 1. Namely, each of them incorporates the inventive concept protecting each and every access to the unencrypted form of the encrypted data according to rules enforced by an access mechanism to ensure that the unencrypted form is not subject to unauthorized access or distribution. For example, claim 24 uses the same language as claim 1 to incorporate this concept. ’409 patent, claims 24. Other independent claim include this inventive concept with a limitation where access to “unprotected

[11] Indeed, billions of people have not felt the need to “re-invent the wheel” since.

form of the protected portions of the data is provided only in accordance with the rules as enforced by an access mechanism, so that unauthorized access to the protected portions of the data is not the unprotected form of the protected portions of the data." *See* '409 patent, claim 21; *see also* claims 25, 30, 32, 33, 36, 38 (reciting similar language).

The other asserted claims are valid under § 101 for additional reasons as well. For example, the Court's constructions make clear that the patent is directed to a specific, advanced method of access/distribution control to digital data through encryption. For example, the parties agreed or the Court ruled that:

1. "means for outputting" has the function of "outputting images represented by the accessed data" / "outputting the output signal represented by the accessed data" and the corresponding structure of an "I/O controller and associated display monitor or printer"

2. "means for generating" has the function of "generating the output signal from the accessed data" and the corresponding structure of an "one or more devices inputting signals into the I/O controller and the I/O controller"

3. "data encrypting key . . . corresponding data decrypting key" means "a key used to encrypt data . . . a key that may be used to decrypt the data encrypted with the data encryption key"

4. "means for storing" / "storage means" has the function of "storing the rules" and the corresponding structure of "computer storage"

5. "means for displaying" has the function of "displaying the images represented by the accessed data" and the corresponding structure of "a display monitor"

6. "access control rights" means "permissions that control a user's access to data"

D.I. 82 at 7.

JPMC tries to cast these claims elements as just conventional and adding nothing to the claims. But this is not true—and JPMC offers no evidence in support of it being true. Again, claims must be read as a whole and, as discussed above, no prohibition on using standard components in order to develop a new invention, especially when those components are used to build a new machine. JPMC wants to just discard all the claim limitations, including those it requested that the Court construe, and proclaim that all that is claimed is the "idea of restricting access to data using a set of rules" or "the idea of controlling access to openly distributed information." If that were actually true (it is not) JPMC would have to concede infringement. That JPMC has not conceded infringement also is an indication that the claims are directed to a specific application and do not claim abstract ideas.

JPMC's other arguments regarding the asserted claims other than claim 1 are inapposite. In each instance JPMC views the claim limitations in isolation, rather than analyzing them as a whole, just as it did for claim 1. Motion at 17-26. This is error. Moreover, in each instance JPMC ignores the inventive concept (discussed above) that each claim is directed to—either expressly (in the case of the independent claims) or implicitly (in the case of the dependent claims that add to the independent claims). Motion at 17-26. This is also error. In the end, JPMC makes all the same analytical errors with respect to the other asserted claims as it did with claim 1—it just repeats them over and over again. JPMC also ignores that the dependent claims further limit the already specific applications in the independent claims, making those claims even more specific and concrete, though not required.

At bottom, JPMC has utterly failed to establish that any claim of the '409 patent claims only an abstract idea. Not even the concepts as described by JPMC—restricting access to data using a set of rules, or continuing to control access to openly distributed information—are abstract. And JPMC cannot manufacture abstractness by ignoring all of the relevant claim language. All of the asserted claims of the '409 patent are directed to a specific cryptographic feature that protects each and every access to the unencrypted form of encrypted data according to rules enforced by an access mechanism.

## C. The ’084 Patent Does Not Claim an Abstract Idea

### 1. The Invention of the ’084 Patent

The ’084 patent covers a network-based system for detecting network intrusions. The patent describes a data collection and processing center, which looks at information from multiple hosts, servers and computer sites. The data is collected and then analyzed by an intrusion analysis unit, referred to as a “data collection and processing center.” If an intrusion is detected, then the center alerts other network devices.

Unlike prior art intrusion detection methods, the ’084 patent uses broad-based network intrusion detection, which analyzes network traffic data from many different sources in the protected networks. This allows the ’084 invention to be more accurate and to detect intrusions in near real-time. The specification contrasts network-based intrusion detection of the invention with conventional intrusion detection systems:

> Conventional intrusion detection systems merely provide indications of already occurred hacker events and attacks. There is no functionality or capability present in conventional intrusion detection systems to determine near-real time adjustments for firewalls, etc. which will solve the problem. Even if a conventional intrusion detection system was improved so that it could adjust firewall parameters based on what it detects, this adjustment would necessarily happen after the attack, and thus be of little value.

’084 patent, 11:63-12:4.

Figure 2 shows an exemplary system: “a plurality of network devices such as hosts, servers, and personal computers attached within customer site networks (shown here as customer site networks 220, 230, 240, 250), are shown coupled to an intervening computer network 204, such as a public network like the Internet.” *Id.* at 6:52-57. The data collection and processing center comprises a firewall 210 and computer system 205. It detects anomalies in the network by using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer cites. *See, e.g.*, *id.* at 14:20-25. The computerized analysis engine uses "pattern correlations across multiple customer's events in order to better determine the occurrence and sources of suspected intrusion-oriented activity prior to actually alarming." *Id.* at 8:28-31. Once an anomaly is detected, the center can alert other components, as well as control them.

### 2. <u>The Claims of the '084 Patent Are Not Directed or Drawn to an Abstract Idea</u>

The '084 patent concerns computer network security and is directed to a specific technique of monitoring computer-network traffic to detect intrusions and reporting such anomalies. Neither idea is abstract. JPMC describes the patent as being directed to "detecting anomalies in multiple data streams and telling people where they are found." Motion at 27. This conceptualization is so concrete it cannot be abstract. Even per JPMC, the patent provides a specific method for detecting and reporting malicious computer network activity based on the monitoring and comparing of traffic in multiple data streams to detect anomalous behavior, then reporting that behavior. This is a novel, innovative, and specific application of network intrusion prevention. "Detecting anomalies in multiple data streams and telling people where they are found" is not a building block of human ingenuity. It is not a fundamental practice. It is not a principle, original cause or motive. It is not a bare mathematical formula or algorithm. The patent claims a specific implementation of the idea that better network security can be achieved by monitoring and comparing traffic from multiple locations, and is not at all like the broad, well known, primary concepts that have been found ineligible under § 101.

For example, the fundamental principles claimed in *Bilski* and *Alice Corp*. were hedging and intermediated settlement, respectively, and ***nothing more***. *Bilski*, 561 U.S. at 611; *Alice*

*Corp.*, 134 S. Ct. at 2355. These were "fundamental economic practice[s] long prevalent in our system of commerce." *Alice Corp.*, 134 S. Ct. at 2356. The same cannot be said here. The patent is generally directed to network security and applies specific methods—network–based intrusion detection—to providing detection of network anomalies. '084 patent, Abstract, 1:1-5. Even network security is not an abstract concept. It is one that is new, brought about only recently as computer networks proliferate throughout all aspects of our society. This was especially true in March 2002, when the patent was filed. Network technology has advanced significantly in the 12 years since the inventors filed for their patent so what might seem commonplace now, was relatively unknown then. And the actual concept at issue here (even as presented by JPMC), using network detection techniques to monitor multiple data streams in order to detect anomalous behavior, then reporting that behavior, is far narrower than network security.

The patent is limited to a specific medium, using networked computer architecture with multiple communication streams, and is limited to a specific method, detecting and reporting anomalies across those multiple streams using network-based intrusion detection and pattern correlations.[12] The specification teaches that this was a new and unique approach to network security. '082 patent at 5:1-14, 44-56. Compared to the age-old concept of hedging at issue in *Bilski*, or *Alice Corp.* where the Court cited an 1896 publication that confirmed the notion of intermediated settlement was known in commerce for over a century, the concept at issue here was untried and innovative. *Alice Corp.*, 134 S. Ct. at 2356 (citing 1896 publication as support

[12] The Court construed the term "network-based intrusion detection" as "techniques for detecting, by analyzing network communications, whether unauthorized computers have entered or are seeking to enter a network, or are conducting reconnaissance activities." D.I. 82 at 5. The Court's claim construction further highlights the technological aspects of the invention and confirms that it claims patent-eligible subject matter.

for proposition that intermediated settlement was a fundamental economic practice long prevalent in our system of commerce).

Most telling, as with each of the patents at issue, JPMC does not argue that the ’084 might preempt an abstract concept, despite it being the paramount concern. JPMC does not raise a pre-emption issue because there is none. The ’084 patent does not cover all ways of securing a network. It does not cover all methods of intrusion detection. It does not cover all ways of using multiple data streams to detect anomalies. Rather, only those systems and methods that use the claimed “network-based intrusion detection techniques” that analyze data across multiple network access points, such as “hosts, servers, and computer sites in a networked computer systems” to detect anomalies could even potentially infringe the ’084 patent. This is a well-defined concrete and meaningful invention, cabined to its claims. It is difficult, then, to understand how the patent could claim an abstract idea, and only an abstract idea, when JPMC itself does not suggest that the patent preempts more than the limited application that is claimed.

Rather, JPMC is concerned that the ’084 patent is directed to an idea. Throughout its brief, it argues that because different ideas underlie the claimed concepts the claims themselves must be ineligible. The entirety of its analysis is limited to only separating the claim limitations into JPMC’s choice snippets, defining them as only pertaining to a “conventional” idea, and declaring the invention to be nothing but an abstraction. Motion at 28-30 (“The *idea* of analyzing traffic coming into multiple hosts or sites is, however, an abstract idea”).[13] But as explained earlier, and as acknowledged by the Supreme Court in *Alice Corp.*, an idea is what kindles every invention. All innovation can be reduced to an idea or collection of ideas. That

[13] Here and elsewhere in its brief JPMC ignores that the ’084 patent is directed to specific methods of traffic analysis and alerting, e.g., network based intrusion detection where devices that are anticipated to be affected by an anomaly are determined by using pattern correlations. ’084 patent, claim 1.

does not make it ineligible or abstract.

JPMC confuses an idea that is abstract with one that is describable in concrete technological terms. By eschewing any analysis into whether the ideas are indeed abstract, JPMC need offer no reasoning other than its own conclusions and attempts to shoehorn in snippets of the claim into inapposite fact patterns. But post-*Alice Corp.*, this Court has been careful to fully analyze the Supreme Court's § 101 jurisprudence and follow the "guideposts" the Court has set out in determining whether an idea is indeed abstract. First, as discussed, network security is not a long-prevalent practice; it is very new and made necessary only by very new technology. This is especially true when considered at the time of the invention.

Second, the claimed method of detecting anomalies on multiple computer network data streams cannot be done in the human mind or by a human using pen and paper. It is not an abstract method. It requires specific network architectures, hardware and software all working together to detect anomalies and protect the system. Data packets traverse multiple points of a network and are reviewed by software. These data packets are a collection of millions, if not billions, of 1's and 0's. Algorithms process and monitor these packets, analyze them using detection protocols, and report anomalies. Even if the data packets were printed out, and reviewed manually, and the algorithms broken down into steps such that a human could review them, it would take enormous manpower and time to even attempt to practice the patent by hand.[14] The point of the system is to monitor network traffic in real time. If an intrusion is

[14] To provide some perspective, a basic home network will operate at 1.5 Mbps. That means 1.5 million bits per second can stream this one network. Most enterprise networks will operate at significantly higher bandwidths and have multiple lines. Further, the patent is concerned with monitoring network traffic across multiple connections. Nevertheless, even assuming the simple case, one would need to review more than 25,000 pages of indecipherable 1's and 0's for just ***one minute*** of network traffic. Reviewing this mountain of paper might play nicely in the theatre of the absurd, but it has no grounding in reality.

detected it has to be stopped immediately, not days later after someone has reviewed and compared the tens of thousands of pages of data. The only step that might be done manually, the final step of reporting an anomaly, can only be done after the system has analyzed the data streams.

Third, the patent does not claim conventional tasks that can be performed without any particular structure or technology. There is nothing conventional about an algorithm using network-based intrusion detection techniques or pattern correlations across multiple data streams. The entire purpose of the patent is that it can only be performed on a specific structure using specific technology.

In *Alice*, the Supreme Court noted that it "need not labor to delimit the precise contours of the abstract ideas category in this case" because intermediated settlement was "squarely within the realm" of that definition. *Alice Corp.*, 134 S.Ct. at 2357. Here, this Court need not labor to delimit the contours either. While hedging or intermediated settlement fall very clearly on one side of the line, providing network security by analyzing and comparing data across multiple communication streams using pattern correlations to spot devices that are affected (or anticipated to be affected) by an anomaly falls very clearly on the other side of the line, just as the concepts underlying all the patents-in-suit do. There are no concerns of pre-emption. The claims, even as described by JPMC, are not directed to a long-standing, fundamental practice. The patent cannot be practiced in the human mind or on pen and paper. The patent does not claim merely conventional activity without regard to a specific structure or technology. The '084 patent simply does not claim an abstract idea.

### 3. <u>Assuming The '084 Patent Claims An Abstract Idea (It Does Not), The Claimed Limitations Recite Significantly More</u>

Because no abstract idea is actually claimed, the Court's analysis need go no further.

*McRO, Inc. v. Atlus U.S.A.*, No. 13-1870, 2014 WL 4772196, at *4-5 (C.D. Cal. Sept. 22, 2014) (describing the *Alice Corp.* test as a one-step process if no abstract concept is found). The second inquiry set forth in *Alice* applies only if the '084 patent claims an abstract idea. *Alice Corp.*, 134 S. Ct. at 2355. Even assuming it did, however, the claims are directed to an innovative concept and require using computer technology in a particular way as to add significantly more, making the claims eligible under § 101. All of JPMC's arguments, on the other hand, are better understood as obviousness arguments. JPMC never disputes that the patent is directed to a specific idea or that it has specific claims that meaningfully apply it. Rather, it argues that because (in its estimation) some of the aspects were "conventional" then the patent is invalid. But here, JPMC uses "conventional" as a stand-in for well-known. Thus, its arguments are misplaced in the context of § 101 and it should have moved for summary judgment on § 103, if it had art, *or any support other than its own conclusions*, that the steps were indeed conventional.

For this step, the Court must then "examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice Corp.*, 134 S. Ct. at 2357 (quoting *Mayo*, 132 S. Ct. at 1294, 1298). The inventive concept is taught in the specification as broad-based network intrusion detection using analysis of aggregate network traffic, which, unlike known intrusion detection which focused on traffic for a single device, allowed better monitoring because more patterns could be spotted and the system therefore could act to detect or even prevent attacks in near-time. '084 patent, Abstract, 1:4-55, 8:45-54, 8:66-9:6, 11:63-12:4. The inventor realized that not only monitoring network traffic across multiple points was important, but then by comparing the traffic using specific "network-based intrusion detection techniques," one was better able to detect a network anomaly. For example, an intrusion into one network could be well disguised to appear as normal traffic. But the intruder's camouflage would be revealed once compared to the network traffic of other systems.

The meaningfulness of the claims is buttressed by the specification's teaching of "a *specific way* of doing something with a computer." *CLS Bank Intern. v. Alice Corp. Pty. Ltd.*, 717 F.3d 1269, 1302 (Fed. Cir. 2013) (emphasis in original).[15] Here the "patent does more than simply instruct" one to perform an abstract idea "on a generic computer." *Alice Corp.*, 124 S. Ct. at 2359. It teaches using a specific system (a secured network with firewall and a plurality of hosts, servers, and computer sites) and methods of monitoring and analyzing data to detect network intrusion. Neither these steps nor the technology itself were "purely conventional" at the time the patent was filed. *See id.*

The limitations add "something more" to the idea of network security, or even network security across multiple data streams. The Court's constructions make clear that the patent is directed to a specific, advanced method of intrusion detection and control. Many of these constructions were agreed upon by the parties, so even JPMC recognized initially the patent was a meaningful application of a specific concept. For example, the parties agreed that:

1. "host" means a "computer"
2. an "intrusion" means "an entry by an unauthorized computer into a secured network"
3. "adjusting the firewall/controlling the device" means "reconfiguring or adjusting the pertinent parameters of the [firewall/device]"
4. "generating an automated response to the intrusion" means

[15] The Supreme Court affirmed in its opinion that one cannot save a claim to an abstract idea by simply stating "apply it with a computer" (*Alice Corp.*, 134 S. Ct. at 2358) and left undisturbed the discussion in Judge Rader's opinion concerning a specific machine.

> "generating a response (including an alert, a log, a parameter adjustment, or a notification) to the intrusion without manual intervention"

D.I. 76-1 at 3. Each of these agreed-on constructions point to a sophisticated, specific type of computer architecture. Similarly, the Court construed "anomaly" as an "irregularity in the data" and "pattern correlations…" as "analysis or patterns of data across multiple hosts, servers, and/or computer sites." D.I. 82 at 5. The constructions require complex algorithms working across this advanced architecture. For example, claim 1 requires a network implementation with "a firewall," and a plurality of "hosts, servers, and computer sites in a networked computer system." Claim 1. Algorithms must be implemented that use "network-based intrusion detection techniques." *Id.* Implicit in this, is that it can function seamlessly over multiple data streams, analyzing the data from each stream and comparing it in real time, no easy task. Once deployed, if the method detects an anomaly over the monitored data streams, the algorithms analyze patterns of data across the multiple hosts, servers, and computer sites. *Id.* Then, a signal or message must be sent alerting the threatened device. These limitations transform any abstract concept into something more. *Card Verification Solutions, LLC v. Citigroup Inc.*, No. 13-6339, 2014 WL 4922524, at *4 (N.D. Ill. Sept. 29, 2014) (finding that claims that included "a computer, nonsecure network, and pseudorandom tag generating software" are more than a mental process and thus not ineligible subject matter).

For purposes of its summary judgment motion, JPMC discards all this under the presumption that these steps were conventional. Much of its argument focuses on asking the Court to ignore claim limitations. For example, JPMC wants the Court to ignore that claim 1 requires a firewall. While this means that the network must be configured in a specific way (again highlighting a lack of pre-emption), JPMC says that a firewall was well known and thus adds nothing to the patent. *Id.* This ignores the teachings of the patent that the existing firewalls were configured in a way that made them highly vulnerable to hacker attacks and that the ’084 invention solved this problem by allowing firewalls to be configured based on the results of the claimed broad-based network detection. *See, e.g.*, ’084 patent, 5:1-5, 6:15-19, claim 15.[16] And JPMC’s sophist reasoning that the patent might just as well have said “printer” (Motion at 28) is dishonest. The firewall is part of the invention, it is in the title, it is in the summary, it is in the independent claims, and it is part and parcel of certain of the dependent claims as well. As explained above, the specification teaches that the firewall filters the packets and assists in the monitoring and analyzing of the data stream. JPMC’s example of a printer, on the other hand, is irrelevant.

Similarly, JPMC denigrates the first step of claim 1 by parsing out limitations and saying that they are conventional. Motion at 29. It thereby ignores the totality of the claim limitation that uses “network-based intrusion detection techniques”[17] in a novel way for the specific claimed system. Contrary to JPMC, this is more than just “an idea” of analyzing traffic. *Id.* Rather, this claim limitation covers collecting, comparing, and analyzing the traffic entering into a plurality of sources (including computers, servers, and computer sites all connected over a secure network with a firewall) to provide a broader base from which to determine if an intrusion has occurred. Far from an abstract idea, this limitation meaningfully applies “network-based intrusion detection system” to a specific implementation. ’084 Patent, Field of the Invention.

[16] JPMC argues that a firewall is not a specific machine. But what definition of “machine” would exclude firewall, described by the patent as “a combination hardware and software buffer that is between the internal network and external devices outside the internal computer network.” ’409 patent, 7:5-11.

[17] The Court construed “network-based intrusion detection techniques” as “techniques for detecting, by analyzing network, whether unauthorized computers have entered or are seeking to enter a network, or are conducting reconnaissance activities.”

Accordingly, contrary to JPMC's assertion, this limitation very much requires a specific apparatus and system to practice the invention.

Step 2 requires using "pattern correlation" to determine where an intrusion has occurred. JPMC does not discuss any of these steps in relation to the claim constructions or the specification. It asks the Court to ignore this limitation as "pure data manipulation." Motion at 30. This ignores that the data is being taken from a physical computer network (specifically comprising "hosts, servers and computer sites"), reviewed and analyzed in a specific manner, then processed to determine which devices are anticipated to be effected, and issue corresponding alerts. Of course, this is not just pure processing of numbers with no result or purpose as JPMC suggests. Similarly, step 3, which requires alerting devices, is another meaningful application of the invention to a specific implementation. The Court has construed this as notifying the device, an associated firewall, or an administrator. Thus, it also necessarily implicates the concrete system that is claimed.

JPMC's arguments sound more in § 103 obviousness rather than trying to sincerely describe to the Court what the claims mean. But even JPMC's self-serving assessment that the '084 patent claims only conventional subject matter fails because it is based on pure attorney argument and is contradicted by the PTO. Despite bearing a clear and convincing burden, JPMC does not even attach a declaration from an expert attesting to whether any of the claimed technologies (let alone the claims as a whole) were indeed conventional in 2002 when the patent was filed. *SRAM Corp. v. AD–II Eng'g, Inc.*, 465 F.3d 1351, 1357 (Fed. Cir. 2006) ("[A] moving party seeking to invalidate a patent at summary judgment must submit such clear and convincing evidence of facts underlying invalidity that no reasonable jury could find otherwise."). Nor does it cite to any prior art, perhaps because the PTO has already rejected so many of its arguments by denying IPR petitions relating to the ’084 patent for most of the asserted claims, including JPMC’s *bête noire*, claim 1. Rather, JPMC uses litigation-driven hindsight and conjecture to argue to the Court that “detecting any anomaly using multiple data streams” is abstract, that the claimed computer network is “generic” and that the claimed network-based intrusion detection techniques are “conventional.” All of these arguments are conclusory, without support, and ignore the true nature of the claimed invention and the limitations.

### 4. The Other Asserted Independent And Dependent Claims of The ’084 Patent Are Also Are Not Directed or Drawn to an Abstract Idea

JPMC offers no new arguments for the remaining claims, simply repeating the same attorney argument for each. Each claim of the patent is limited to a specific medium, using networked computer architecture with multiple communication streams, and is limited to a specific method, detecting and reporting anomalies across those multiple streams. If the Court finds that claim 1 is not abstract, then by JPMC’s own argument the remaining claims cannot be as well. None of the remaining claims are directed to an abstract idea, as already discussed above. JPMC raises no pre-emption concern with any of the additional claims. Indeed, many of these claims are dependent claims and thus raise even less threat of pre-emption than claim 1. Similarly, these claims all add different meaningful limitations. The claims are not conventional and JPMC offers no evidence to suggest otherwise.

The ’084 patent claims a novel, useful, and specific application of network-based intrusion detection by collecting and analyzing data across multiple data streams in a secured network to detect an intrusion. This is not abstract.

## IV. CONCLUSION

For at least these reasons, JPMC’s motion should be denied.

Dated: November 3, 2014

DUNNEGAN & SCILEPPI LLC

By __s/Richard Weiss__
Richard Weiss (RW4039)
rw@dunnegan.com
350 Fifth Avenue
New York, New York 10118
(212) 332-8300

-and-

FEINBERG DAY ALBERTI & THOMPSON LLP
Ian Feinberg (Cal. Bar No. 88324)
ifeinberg@feinday.com
Elizabeth Day (Cal Bar No. 177125)
eday@feinday.com
Marc Belloli (Cal Bar No. 224290)
mbelloli@feinday.com
1600 El Camino Real, Suite 280
Menlo Park, CA 94025
Direct: 650-618-4360
Fax: 650-618-4368
(pro hac vice)

Attorneys for Plaintiff